Extension of Overbeck's attack for Gabidulin-based cryptosystems

Horlemann-Trautmann, Anna-Lena ; Marshall, Kyle ; Rosenthal, Joachim

Abstract: Cryptosystems based on codes in the rank metric were introduced in 1991 by Gabidulin, Paramanov, and Tretjakov (GPT) and have been studied as a promising alternative to cryptosystems based on codes in the Hamming metric. In particular, it was observed that the combinatorial solution for solving the rank analogy of the syndrome decoding problem appears significantly harder. Early proposals were often made with an underlying Gabidulin code structure. Gibson, in 1995, made a promising attack which was later extended by Overbeck in 2008 to cryptanalyze many of the systems in the literature. Improved systems were then designed to resist the attack of Overbeck and yet continue to use Gabidulin codes. In this paper, we generalize Overbeck's attack to break the GPT cryptosystem for all possible parameter sets, and then extend the attack to cryptanalyze particular variants which explicitly resist the attack of Overbeck.

DOI: https://doi.org/10.1007/s10623-017-0343-7

Extension of Overbeck's Attack for Gabidulin-based Cryptosystems*

Anna-Lena Horlemann-Trautmann[1], Kyle Marshall[2] and Joachim Rosenthal[2]

[1]EPF Lausanne, Switzerland
[2]Universität Zürich, Switzerland

January 5, 2016

Abstract

Cryptosystems based on codes in the rank metric were introduced in 1991 by Gabidulin, Paramanov, and Tretjakov (GPT) and have been studied as a promising alternative to cryptosystems based on codes in the Hamming metric. In particular, it was observed that the combinatorial solution for solving the rank analogy of the syndrome decoding problem appears significantly harder. Early proposals were often made with an underlying Gabidulin code structure. Gibson, in 1995, made a promising attack which was later extended by Overbeck in 2008 to cryptanalyze many of the systems in the literature. Improved systems were then designed to resist the attack of Overbeck and yet continue to use Gabidulin codes. In this paper, we generalize Overbeck's attack to break the GPT cryptosystem for all possible parameter sets, and then generalize the attack to cryptanalyze particular variants which explicitly resist the attack of Overbeck.

1 Introduction

Cryptosystems based on the hardness of the general decoding problem have received much attention because of their applications to post-quantum cryptography. The practical implementation of these systems, however, has suffered from the drawback of having a large key size relative to RSA or elliptic curve cryptography (ECC). Regardless, coding based cryptography remains one of the most feasible alternatives to traditional number theoretic cryptosystems for resisting quantum attacks such as Shor's factoring algorithm. A large body of work has been produced in the study of cryptography based on codes in the Hamming metric, starting with McEliece in 1978 [14]. It was observed that the cryptosystem he designed had efficient encryption and decryption procedures, however, the proposed public key sizes were significantly larger than keys for RSA or ECC, rendering the system infeasible in its original form.

*This work was supported by SNF grant no. 149716.

The large size of the key in the McEliece cryptosystem is a consequence of the efficiency of combinatorial solutions to the general decoding problem for codes in the Hamming metric. The impetus for interest in codes in the rank metric were preliminary results concerning the rank syndrome decoding problem, in which the best algorithms were of significantly higher complexity [2, 16]. This indicated that cryptosystems could be designed with far smaller parameters than those in the Hamming metric. Cryptosystems based on codes in the rank metric were introduced earlier by Gabidulin, Paramonov, and Tretjakov (GPT) [5]. Since then, proposals for designs of cryptosystems have alternately been attacked and modified. The designs are often based on Gabidulin codes–the rank metric analogy of generalized Reed-Solomon codes–because of the scarcity of efficiently decodable codes in the rank metric. This has led to efficient structural attacks [9, 17] and subsequently improvements in the designs of these codes and their parameters [12, 4, 18, 13]. It should be noted that unlike the syndrome decoding problem in the Hamming metric, the rank syndrome decoding problem is not known to be NP-hard. Other related work has been done in improving algorithms for the rank syndrome decoding problem [7], and also designing rank-metric based cryptosystems which do not rely on Gabidulin codes [8].

The original GPT cryptosystem had its first significant attack by Gibson [9]. Following Gibson's lead, Overbeck proposed an alternative attack that led to a polynomial time break for many parameters of the GPT cryptosystem [17]. In the wake of these developments, two modifications, designed to use Gabidulin codes and yet resist the attack of Overbeck, stand out. They follow a similar idea - a more careful choice of distortion matrix - but have different approaches. The approach taken in [13] is based on enlarging the distortion matrix but restricting its rank, whereas the idea in [18] is based on careful design of the structure of the distortion matrix. While the ideas in these modifications are not necessarily mutually exclusive, an disadvantage of the former version is that it requires a large increase in the public key size in order to be secure against Overbeck's attack. A disadvantage of the latter version is that the distortion matrices must necessarily be quite structured.

In this paper we present a new attack which can be seen as a generalization of Overbeck's, and which allows us to cryptanalyze the systems presented in [18] and [13]. The paper is organized as follows: Section 2 provides some terminology as well as the necessary background regarding rank metric codes and the GPT cryptosystem and its variants. Section 3 provides some basic results that we will need to describe our attack. In particular, we need some basic results about Moore matrices as well as the behavior of matrices under the coordinate-wise Frobenius map. Section 4 outlines the attack on the GPT cryptosystem and Section 5 uses the method to cryptanalyze the aforementioned variants.

2 Background

Let $\mathbb{F} \subset \mathbb{E}$ be two fields with $[\mathbb{E}\colon \mathbb{F}] = m$. We will refer to the rank in the following ways. Given a matrix M with coefficients in $\mathbb{E}$, we mean by the rank of M, the usual notion

of the dimension of the row span of M as a vector space over $\mathbb{E}$. We will denote the row span of a matrix M over $\mathbb{E}$ by $\langle M \rangle$. By column rank (over $\mathbb{F}$) of a matrix M with coefficients in $\mathbb{E}$, we mean the rank of the column span of M as an $\mathbb{F}$-vector space and we will denote this by $\mathrm{colrk}(M)$. When we say the rank of a vector, $\boldsymbol{x} \in \mathbb{E}^n$, we mean the $\mathbb{F}$-rank of the matrix obtained by expanding $\boldsymbol{x}$ into an $m \times n$ matrix according to some basis of $\mathbb{E}$ over $\mathbb{F}$. The rank defined in this way is invariant with respect to the choice of basis. An equivalent way to express the rank of a vector $\boldsymbol{x} \in \mathbb{E}^n$ is to take the dimension over $\mathbb{F}$ of the subspace of $\mathbb{E}$ which is spanned by the coordinates of $\boldsymbol{x}$.

If we are working over a base field $\mathbb{F} = \mathbb{F}_q$ of cardinality q, and an extension field $\mathbb{E} = \mathbb{F}_{q^m}$, then we denote by $[i]$ the ith Frobenius power, q^i. The Frobenius map can be applied to a matrix or vector coordinate-wise. If $M = (M_{a,b})$ is any matrix (or vector) over $\mathbb{F}_{q^m}$, we define $M^{([i])} = (M_{a,b}^{[i]})$. It is easy to verify that $\langle M \rangle^{([i])} = \{\boldsymbol{x}^{([i])} \mid \boldsymbol{x} \in \langle M \rangle\} = \langle M^{([i])} \rangle$.

Definition 2.1. The *rank distance* between $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ is defined to be

$$d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{rk}(\boldsymbol{x} - \boldsymbol{y}).$$

This defines a metric on $\mathbb{F}_{q^m}^n$. If V is a subspace of $\mathbb{F}_{q^m}$, the *minimum rank distance* of V is given by

$$d_{\mathrm{R}}^{\min}(V) = \min\{d_{\mathrm{R}}(\boldsymbol{x}, 0) \mid \boldsymbol{x} \in V\}.$$

We will also use the term *weight* of $\boldsymbol{x}$, denoted by $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{x})$, to mean $d_{\mathrm{R}}(\boldsymbol{x}, 0)$.

The Singleton bound for (linear) rank-metric codes is given by the inequality (see e.g. [3])

$$d_{\mathrm{R}}^{\min}(V) \leq n - \dim(V) + 1.$$

Definition 2.2. A rank-metric code meeting the Singleton bound is called a *maximum rank-distance (MRD) code.*

The linear isometries of $\mathbb{F}_{q^m}^n$ with respect to the rank metric are given by $(\mathbb{F}_{q^m}^*) \times \mathrm{GL}_n(\mathbb{F}_q)$ [1]. Throughout the paper we will make extensive use of the coordinate-wise Frobenius map. This map is a semi-linear isometry of the rank-metric with many useful properties. For more information on semi-linear isometries, see [15].

Definition 2.3. A matrix $M \in \mathbb{F}_{q^m}^{k \times n}$ is called a *Moore matrix* if there exists a $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^n$ such that row i of M is equal to $\boldsymbol{\alpha}^{([i-1])}$ for $i = 1, \ldots, k$. $\boldsymbol{\alpha}$ is called the generator of M.

In the following lemma, we will summarize some of the important properties of Moore matrices. These results are known or are direct consequences of known results.

Lemma 2.4. *Fix $k \leq N$, and let $M \in \mathbb{F}_{q^m}^{k \times N}$ be a Moore matrix with generator $\boldsymbol{\alpha}$, with $\mathrm{rk}(\boldsymbol{\alpha}) = n \leq N$.*

1. *If $k \leq n$, then $\langle M \rangle$ has dimension k, and minimum rank distance $n - k + 1$.*
2. *If $k < n$, then $\dim(\langle M \rangle \cap \langle M \rangle^{(q)}) = k - 1$ and $\dim(\langle M \rangle + \langle M \rangle^{(q)}) = k + 1$.*

3. *If $A \in \mathbb{F}_{q^m}^{k\times N}$ is another Moore matrix then $M+A$ is also a Moore matrix. Moreover, if the column rank of A is equal to $r < n-k+1$, then the minimum rank distance of $\langle M+A\rangle$ is at least $n-k+1-r$.*

4. *If the minimum rank distance of $\langle M\rangle$ is $d > 1$, then the minimum rank distance of $\langle M\rangle + \langle M^{([1])}\rangle$ is equal to $d-1$.*

5. *If the minimum rank distance of $\langle M\rangle$ is $d > 1$, and $E \in \mathbb{F}_q^{N\times(N-s)}$ is a full rank matrix, then ME is a Moore matrix and the minimum rank distance of $\langle ME\rangle = \langle M\rangle E$ is at least $d-s$.*

Proof. 1. The case $n = N$ is given in Theorems 6 and 7 of [3]. Thus we know that, if $N > n$, we can puncture the vector space $\langle M\rangle$ to get a space $\langle M'\rangle$ of length n, dimension k and minimum rank distance $n-k+1$. Hence the minimum rank distance of $\langle M\rangle$ is at least $n-k+1$. That it cannot be greater follows from Lemma 4.7 of [11].

2. The first statement follows easily from the Moore matrix structure. This implies that

$$\dim(\langle M\rangle + \langle M^{(q)}\rangle) = \dim(\langle M\rangle) + \dim(\langle M^{(q)}\rangle) - \dim(\langle M\rangle \cap \langle M\rangle^{(q)}) = k+1.$$

3. The first statement follows from the fact that $(x+y)^{[i]} = x^{[i]}+y^{[i]}$ for any $x, y \in \mathbb{F}_{q^m}$. Therefore the Moore structure is preserved under addition of matrices. For the second part note that any element $\boldsymbol{a} \in \langle A\rangle$ has rank at most r and any non-zero element $\boldsymbol{m}_i \in \langle M\rangle$ has rank at least $n-k+1$. Hence $\boldsymbol{a}$ can change the rank of $\boldsymbol{m} \pm \boldsymbol{a}$ by at most r, i.e. the rank of any non-zero element of $\langle M+A\rangle$ has rank at least $n-k+1-r$.

4. Since the minimum rank distance of $\langle M\rangle$ is $d > 1$, it follows from 2. that $\dim(\langle M\rangle + \langle M^{([1])}\rangle) = k+1$. Then part 1. implies that the minimum rank distance of $\langle M\rangle + \langle M^{([1])}\rangle$ is $n-(k+1)+1 = d-1$.

5. Let $E' \in \mathbb{F}_q^{n\times s}$ be such that $[E \mid E']$ has full rank. Then, $[E \mid E']$ is an isometry, and so $\langle G[E \mid E']\rangle$ has minimum rank distance d. Removing the last s columns gives $\langle GE\rangle$, which can only decrease the rank by at most s.

□

A well-known class of codes in the rank metric are the Gabidulin codes [3]. Gabidulin codes are those whose generator matrix is a Moore matrix in which the generating vector has full rank:

Definition 2.5. Fix $k \le n \le m$, and let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, $\mathrm{rk}(\boldsymbol{\alpha}) = n$. The *Gabidulin code* of length n and dimension k over $\mathbb{F}_{q^m}$, denoted by $\mathrm{Gab}_{n,k}(\alpha)$ is given by

the row space of the matrix,

$$G = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^{[1]} & \alpha_2^{[1]} & \dots & \alpha_n^{[1]} \\ & & \vdots & \\ \alpha_1^{[k-1]} & \alpha_2^{[k-1]} & \dots & \alpha_n^{[k-1]}. \end{pmatrix}. \tag{1}$$

From Lemma 2.4, we have that Gabidulin codes are MRD codes. Moreover, they have efficient decoding algorithms [20, 21, 3]. Gabidulin codes are also closed under the linear isometries of the rank-metric (for isometries of rank-metric codes see e.g. [1, 15]). Specifically, if $\beta \in \mathbb{F}_{q^m}^*$ and $\sigma \in \mathrm{GL}_n(\mathbb{F}_q)$, then $\beta \mathrm{Gab}_{n,k}(\boldsymbol{\alpha})\sigma = \mathrm{Gab}_{n,k}(\beta \boldsymbol{\alpha} \sigma)$.

2.1 Decoding From an Arbitrary Generator Matrix

McEliece cryptosystems based on Generalized Reed-Solomon (GRS) codes were effectively broken by Sidel'nikov-Shestakov [19]. Their attack allows one to recover the generating vector of a GRS code, and therefore a decoding algorithm. Similarly, in the case of Gabidulin codes, a decoding algorithm can be found if one knows the canonical generator matrix of the code. Using a simple method, we can also recover a decoding algorithm if the generator matrix is not in canonical form, as described in the following.

Consider the Gabidulin code $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$ with dimension $1 < k < n$ and generator matrix SG, where $S \in \mathrm{GL}_k(\mathbb{F}_{q^m})$ and G of the form (1). Then $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})^{([1])} \cap \mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$ is the Gabidulin code $\mathrm{Gab}_{n,k-1}(\boldsymbol{\alpha}^{([1])})$ (see Lemma 2.4). Iterating with this new Gabidulin code, we can eventually obtain a code of dimension 1, which is generated by $\boldsymbol{\alpha}^{([k-1])}$. If we take some non-zero element of this space, it has the form $\beta \boldsymbol{\alpha}^{([k-1])}$, for some $\beta \in \mathbb{F}_{q^m}$. Applying the Frobenius map coordinate-wise $m - k + 1$ times, we obtain an element of the form $\beta^{[m-k+1]}\boldsymbol{\alpha}$. Using this element, we can construct a generator matrix, BG, for $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$ which will have the form

$$BG = \begin{pmatrix} \beta^{[m-k+1]} & & & \\ & \beta^{[m-k+2]} & & \\ & & \ddots & \\ & & & \beta \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^{[1]} & \alpha_2^{[1]} & \dots & \alpha_n^{[1]} \\ & & \vdots & \\ \alpha_1^{[k-1]} & \alpha_2^{[k-1]} & \dots & \alpha_n^{[k-1]} \end{pmatrix}.$$

The change of basis from SG to BG is then given by BS^{-1}. For a message $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$, encoded as $\boldsymbol{m}SG$, we can now decode with respect to $\mathrm{Gab}_{n,k}(\beta^{[m-k+1]}\boldsymbol{\alpha})$ to obtain $\boldsymbol{m}SB^{-1}$. Then, applying BS^{-1}, we can recover $\boldsymbol{m}$.

2.2 GPT and GGPT Cryptosystems

Let $S \in \mathrm{GL}_k(\mathbb{F}_{q^m})$, $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a Gabidulin code, say $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$, capable of correcting t' errors, and $X \in \mathbb{F}_{q^m}^{k \times n}$ be a matrix of column rank $t < t'$. We define

$$G_{\mathrm{pub}} := SG + X. \tag{2}$$

We call a *GPT cryptosystem* one in which the public key is given by the pair

$$\kappa_{\text{pub}} = (G_{\text{pub}}, t' - t), \tag{3}$$

and the private key is given by

$$\kappa_{\text{pvt}} = (G, S). \tag{4}$$

An encryption of a message $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$ is given by

$$\boldsymbol{m}G_{\text{pub}} + \boldsymbol{e} = \boldsymbol{m}SG + \boldsymbol{m}X + \boldsymbol{e},$$

where $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ is a randomly chosen vector of rank at most $t' - t$. The product $\boldsymbol{m}S$ can be recovered from a decoding algorithm for $\text{Gab}_{n,k}(\boldsymbol{\alpha})$ because all elements of $\langle X \rangle$ have weight at most t. Specifically, if $\text{wt}_{\text{R}}(\boldsymbol{e}) \leq t' - t$,

$$\text{wt}_{\text{R}}(\boldsymbol{m}X + \boldsymbol{e}) \leq \text{wt}_{\text{R}}(\boldsymbol{m}X) + \text{wt}_{\text{R}}(\boldsymbol{e}) \leq t'.$$

Inverting S, the message $\boldsymbol{m}$ can then be recovered. We will call the elements of the form $\boldsymbol{m}X$ the *designed error* associated with the encryption of $\boldsymbol{m}$, and X the *designed error matrix*.

In [18, 13] the authors consider an alternative version which we call the *generalized GPT (GGPT) cryptosystem*. This system uses a public matrix of the form

$$\hat{G}_{\text{pub}} := S[X \mid G]\sigma \in \mathbb{F}_{q^m}^{k \times (n+\hat{t})}, \tag{5}$$

where G is as before, $X \in \mathbb{F}_{q^m}^{k \times \hat{t}}$ is a matrix of column rank $\hat{t}$, $S \in \text{GL}_k(\mathbb{F}_{q^m})$, and $\sigma \in \text{GL}_{n+\hat{t}}(\mathbb{F}_q)$. The public key is given by

$$\kappa_{\text{pub}} = (\hat{G}_{\text{pub}}, t'), \tag{6}$$

and the private key is given by

$$\kappa_{\text{pvt}} = (G, S, \sigma). \tag{7}$$

In the GGPT cryptosystem, an encryption of $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$ is given by

$$\boldsymbol{m}\hat{G}_{\text{pub}} + \boldsymbol{e},$$

with $\text{rk}(\boldsymbol{e}) \leq t'$. To recover $\boldsymbol{m}$, one first computes

$$(\boldsymbol{m}\hat{G}_{\text{pub}} + \boldsymbol{e})\sigma^{-1},$$

and then ignores the first $\hat{t}$ coordinates. Decoding the last n coordinates with respect to $\text{Gab}_{n,k}(\boldsymbol{\alpha})$, one obtains $\boldsymbol{m}S$, and by applying S^{-1}, the message $\boldsymbol{m}$ can be recovered.

2.3 Overbeck's Attack

We will describe Overbeck's attack from [17] for the case of the GGPT cryptosystem; the attack for the GPT case is analogous. Let $G \in \mathbb{F}_{q^m}^{k\times n}$ be a generator matrix for the Gabidulin code, $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$. The first step in Overbeck's attack is to consider the extended matrix (for some $u \geq 1$)

$$G_{\mathrm{ext}} := \begin{pmatrix} S[X \mid G]\sigma \\ (S[X \mid G]\sigma)^{([1])} \\ \vdots \\ (S[X \mid G]\sigma)^{([u])} \end{pmatrix} = \tilde{S} \left(\begin{array}{c|c} X & G \\ X^{([1])} & G^{([1])} \\ \vdots & \vdots \\ X^{([u])} & G^{([u])} \end{array}\right) \sigma.$$

Since the n right-most columns of $G_{\mathrm{ext}}\sigma^{-1}$ span the Gabidulin code $\mathrm{Gab}_{k+u}(\boldsymbol{\alpha})$, the matrix can be brought into the form of

$$G'_{\mathrm{ext}} = \tilde{S}' \left(\begin{array}{c|c} X^* & G^* \\ X^{**} & 0 \end{array}\right) \sigma, \tag{8}$$

by some suitable row transformation, where $X^* \in \mathbb{F}_{q^m}^{(k+u)\times \hat{t}}$, $G^* \in \mathbb{F}_{q^m}^{(k+u)\times n}$ is a generator matrix of $\mathrm{Gab}_{k+u}(\boldsymbol{\alpha})$, and $X^{**} \in \mathbb{F}_{q^m}^{(k-1)u\times \hat{t}}$. If X^{**} has rank $\hat{t}$, then any element of $\langle G'_{\mathrm{ext}}\rangle^{\perp} = \langle G_{\mathrm{ext}}\rangle^{\perp}$ has the form $\sigma^{-1}[0 \mid \boldsymbol{h}]$, where $\boldsymbol{h} \in \mathrm{Gab}_{k+u}(\boldsymbol{\alpha})^{\perp}$. With this information one can reconstruct the code $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$ and recover the encrypted message.

In the case when X^{**} does not have full rank, Overbeck's attack fails, since $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$ cannot be reconstructed from the dual of $\langle G_{\mathrm{ext}}\rangle^{\perp}$. This is why, in [13], Loidreau suggests to use a randomly chosen X of low rank, a, since then the rank of X^{**} can be bounded above. Specifically, to resist Overbeck's attack, one should choose $\hat{t} > (n-k)a$. However, this would drastically increase the key size of the cryptosystem. To avoid this problem of large key size, the Smart Approach considered in [18], is to design X in a structured way so that X^{**} is rank-deficient, without necessarily having to increase $\hat{t}$. However the structure of X makes the Smart Approach more vulnerable to attacks. A more detailed description of these two systems is given in Section 5.

3 Preliminary Results

In this section, we show that one can decompose a matrix (or vector) of low column rank into the product of two matrices, one of which has full column rank, and the other with elements restricted to $\mathbb{F}_q$. Moreover, we prove some results about the coordinate-wise Frobenius map, as well as the structure of the designed error matrix, which we will need later on in our attack.

We will denote by $M_{t\times n,r}(\mathbb{F}_q)$ the set of $t \times n$ matrices over $\mathbb{F}_q$ with rank r. The sphere around the origin of rank radius t in $\mathbb{F}_{q^m}^n$ will be denoted by

$$S_{n,t}^{\mathrm{R}}(\mathbb{F}_{q^m}) := \{\boldsymbol{x} \in \mathbb{F}_{q^m}^n \mid \mathrm{rk}(\boldsymbol{x}) = t\}.$$

Proposition 3.1.

$$S^{\mathrm{R}}_{n,t}(\mathbb{F}_{q^m}) \cong S^{\mathrm{R}}_{t,t}(\mathbb{F}_{q^m}) \times M_{t\times n,t}(\mathbb{F}_q)/\mathrm{GL}_t(\mathbb{F}_q),$$

where $M_{t\times n,t}(\mathbb{F}_q)/\mathrm{GL}_t(\mathbb{F}_q)$ is the set of equivalence classes of $t \times n$ matrices over $\mathbb{F}_q$ of rank t, where two matrices are equivalent if they have the same row span.

Proof. As representatives of the cosets in $M_{t\times n}(\mathbb{F}_q)/\mathrm{GL}_t(\mathbb{F}_q)$ we consider the reduced row echelon form of the respective row span of the elements of the coset. Define the map

$$\begin{aligned}\varphi\colon S^{\mathrm{R}}_{t,t}(\mathbb{F}_{q^m}) \times M_{t\times n}(\mathbb{F}_q)/\mathrm{GL}_t(\mathbb{F}_q) &\longrightarrow S^{\mathrm{R}}_{n,t}(\mathbb{F}_{q^m})\\ (\boldsymbol{v}, U) &\longmapsto \boldsymbol{v}U.\end{aligned}$$

We now show that φ is bijective.

We first show that φ is surjective. For this consider an arbitrary element in the image of φ, i.e. a vector $\boldsymbol{x} \in \mathbb{F}^n_{q^m}$ of rank t, and let $x_{i_1}, \ldots, x_{i_t}$ be the first t independent entries of $\boldsymbol{x}$, in positions $i_1, \ldots, i_t$. Then, the remaining $n - t$ entries of $\boldsymbol{x}$ can be expressed as an $\mathbb{F}_q$-linear combination of $x_{i_1}, \ldots, x_{i_t}$, thus we can write $\boldsymbol{x} = (x_{i_1}, \ldots, x_{i_t})M$ for some matrix $M \in \mathbb{F}_q^{t\times n}$. Then there exists $S \in \mathrm{GL}_t(\mathbb{F}_q)$ such that $U = S - M$ is in reduced row echelon form. We get $(x_{i_1}, \ldots, x_{i_t})S \in S^{\mathrm{R}}_{t,t}(\mathbb{F}_{q^m})$ and $\boldsymbol{x} = \varphi((x_{i_1}, \ldots, x_{i_t})S, U)$, thus φ is surjective.

To show injectivity, suppose that there are two preimages, i.e. $\boldsymbol{x} = \varphi(\boldsymbol{v}, U) = \varphi(\boldsymbol{v'}, U')$. Without loss of generality, we can assume that $U = [I_t \mid *]$. Denote by U'_j the jth column of U'. Then we have

$$(x_1, \ldots, x_t) = \boldsymbol{v} = (\boldsymbol{v'}U'_1, \ldots, \boldsymbol{v'}U'_t).$$

Since $\boldsymbol{v}$ has rank t, $U'_1, \ldots, U'_t$ must be non-zero. Because U' is in reduced row echelon form, we get $U' = [I_t \mid *]$ and hence

$$(x_1, \ldots, x_t) = \boldsymbol{v} = \boldsymbol{v'}.$$

We furthermore have $x_j = \boldsymbol{v}U_j = \boldsymbol{v'}U'_j$ for $j = t + 1, \ldots, n$. Thus

$$\boldsymbol{v}U_j = \boldsymbol{v'}U'_j \iff \boldsymbol{v}U_j = \boldsymbol{v}U'_j \iff \boldsymbol{v}(U_j - U'_j) = 0.$$

Since $\mathrm{rk}(\boldsymbol{v}) = t$, we get $U_j - U'_j = 0$ for $j = t + 1, \ldots, n$. Thus $U = U'$ and we have shown that φ is injective. □

One can think of the space $M_{t\times n,t}(\mathbb{F}_q)/\mathrm{GL}_t(\mathbb{F}_q)$ as a set of matrices parameterizing the Grassmannian $\mathrm{Gr}(t, \mathbb{F}^n_q)$, i.e. the space of t-dimensional subspaces of $\mathbb{F}^n_q$. According to the proof of Proposition 3.1, we can express a vector $\boldsymbol{x}$ of rank t as $\boldsymbol{x} = \hat{\boldsymbol{x}}U$ for any matrix representation U of a certain element of the Grassmannian $\mathrm{Gr}(t, \mathbb{F}^n_q)$.

We can easily extend the result of Proposition 3.1 from vectors of rank t to matrices of column rank t. Then we get the following result.

Corollary 3.2. *Let $X \in \mathbb{F}_{q^m}^{k\times n}$ be a matrix of rank k and column rank t. Then there exist $V \in \mathbb{F}_{q^m}^{k\times t}$ with $\mathrm{rk}(V) = k$ and $U \in \mathbb{F}_q^{t\times n}$ with $\mathrm{rk}(U) = t$, such that*

$$X = VU.$$

Definition 3.3. Let $X \in \mathbb{F}_{q^m}^{k\times n}$ be a matrix of rank k and column rank t and $V \in \mathbb{F}_{q^m}^{k\times t}, U \in \mathbb{F}_q^{t\times n}$ such that $X = VU$. We call $\langle U\rangle$ the *Grassmann support* of X which will be denoted by $\langle U\rangle = \mathrm{supp}_{\mathrm{Gr}}(X)$. By abuse of notation we will also call any matrix representation $U \in \mathbb{F}_q^{t\times n}$ of this space the Grassmann support of X.

Lemma 3.4. *Let $X \in \mathbb{F}_{q^m}^{k\times n}$ be a matrix of rank k and column rank $t \geq k$. Then $\langle X\rangle \subseteq \mathrm{supp}_{\mathrm{Gr}}(X)$ and the inclusion is strict if and only if $t > k$.*

Proof. Let $U \in \mathbb{F}_q^{t\times n}$ be the Grassmann support of X. By Corollary 3.2, we can write $X = VU$ for some $V \in \mathbb{F}_{q^m}^{k\times t}$. Thus every row of X is a $\mathbb{F}_{q^m}$-linear combination of the rows of U, which implies that $\langle X\rangle \subseteq \langle U\rangle$. Since $\dim(\langle U\rangle) = t$ and $\dim(\langle X\rangle) = k$, we get equality if and only if $k = t$. □

The following two lemmas are needed to prove the main results of this section in Theorems 3.7 and 3.10.

Lemma 3.5. *Let $X \in \mathbb{F}_{q^m}^{k\times n}$ be a matrix of column rank t and $S \in \mathrm{GL}_k(\mathbb{F}_{q^m})$. Then, SX also has column rank t.*

Proof. Denote the ith column of X by X_i. Assume that SX has column rank less than t, i.e. for any $i_1 < \cdots < i_t \in \{1, \ldots, n\}$ there exist $a_1, \ldots, a_t \in \mathbb{F}_q$ such that

$$\sum_{\ell=1}^{t} a_\ell (SX)_{i_\ell} = 0 \iff S\sum_{\ell=1}^{t} a_\ell X_{i_\ell} = 0 \iff \sum_{\ell=1}^{t} a_\ell X_{i_\ell} = 0.$$

This is a contradiction to the fact that the column rank of X is t. □

The following properties of the coordinate-wise Frobenius map will be used throughout the paper. The first statement follows straightforwardly from the $\mathbb{F}_q$-linearity of the Frobenius map, the second and the third are known and can be found, for instance, in [10, 11].

Lemma 3.6. *The following hold for any prime power q and $0 < n \leq m$.*

1. *Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ have rank r. Then, $\boldsymbol{x}^{(q)}$ also has rank r.*
2. *Let $M \in \mathrm{GL}_n(\mathbb{F}_{q^m})$. Then, $(M^{-1})^{(q)} = (M^{(q)})^{-1}$.*
3. *Let $\mathcal{S} \subset \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-subspace. Then, $\mathcal{S}^{(q)} = \mathcal{S}$ if and only if $\mathcal{S}$ has a basis contained in $\mathbb{F}_q^n$.*

We saw in Lemma 3.4 that if a matrix X, with Grassmann support U, has column rank which is greater than its rank, then $\langle X\rangle \subsetneq \langle U\rangle$. The following theorem shows that we can use the Frobenius map to recover $\langle U\rangle$ from X.

Theorem 3.7. *Let $X \in \mathbb{F}_{q^m}^{k\times n}$ be a matrix of column rank s. Then, for any $\ell \geq 0$,*

$$\sum_{i=0}^{s-1}\langle X\rangle^{([i])} = \sum_{i=0}^{s+\ell}\langle X\rangle^{([i])} = \mathrm{supp}_{\mathrm{Gr}}(X).$$

In particular,

$$\dim\left(\sum_{i=0}^{s-1}\langle X\rangle^{([i])}\right) = s.$$

Proof. The chain of subspaces

$$\langle X\rangle \subseteq \langle X\rangle + \langle X\rangle^{(q)} \subseteq \sum_{i=0}^{2}\langle X\rangle^{([i])} \subseteq \dots$$

must eventually stabilize. Let ℓ be such that,

$$\sum_{i=0}^{\ell-1}\langle X\rangle^{([i])} = \sum_{i=0}^{\ell}\langle X\rangle^{([i])}.$$

Define $s' := \dim\sum_{i=0}^{\ell-1}\langle X\rangle^{([i])}$. We have

$$\left(\sum_{i=0}^{\ell-1}\langle X\rangle^{([i])}\right)^{(q)} = \sum_{i=1}^{\ell}\langle X\rangle^{([i])} \subseteq \sum_{i=0}^{\ell}\langle X\rangle^{([i])} = \langle X\rangle^{([\ell])} + \sum_{i=0}^{\ell-1}\langle X\rangle^{([i])}.$$

By Lemma 2.4, $\dim\sum_{i=0}^{\ell-1}\langle X\rangle^{([i])} = \left(\dim\sum_{i=0}^{\ell-1}\langle X\rangle^{([i])}\right)^{(q)} = s'$. Hence, we must have

$$\left(\sum_{i=0}^{\ell-1}\langle X\rangle^{([i])}\right)^{(q)} = \sum_{i=0}^{\ell-1}\langle X\rangle^{([i])},$$

and therefore we can use the third point of Lemma 3.6 and express the sum on the right as the row space of a matrix $U' \in \mathbb{F}_q^{s'\times n}$ of (column) rank s'. Thus there exists $S \in \mathrm{GL}_{k\ell}(\mathbb{F}_{q^m})$ such that

$$\begin{pmatrix} X \\ X^{([1])} \\ \vdots \\ X^{([\ell-1])} \end{pmatrix} = S\begin{pmatrix} U' \\ 0 \end{pmatrix}.$$

This implies that $\langle X\rangle \subseteq \langle U'\rangle$. It follows from Proposition 3.1 that $s' \geq s$. Moreover, by Lemma 3.5, the above matrix on the left has column rank s'. Since, by the $\mathbb{F}_q$-linearity of the Frobenius, the column rank of this matrix is equal to the column rank of X we get $s = s'$ and hence $\mathrm{supp}_{\mathrm{Gr}}(X) = \langle U'\rangle$. ∎

Note that a matrix $X \in \mathbb{F}_{q^m}^n$ can always be decomposed into a Moore matrix component X_{Moore} and a non-Moore matrix component Z as

$$X = X_{\text{Moore}} + Z.$$

Definition 3.8. We will call such a decomposition a *Moore decomposition*. There exists a Moore decomposition so that the non-Moore component has lowest possible column rank. In this case, we call the Moore decomposition a *minimum column rank Moore decomposition*.

Proposition 3.9 shows that, regardless of the choice of Moore decomposition, the Grassmann support of a non-Moore matrix component of a minimum column rank Moore decomposition is the same.

Proposition 3.9. *Suppose that $X \in \mathbb{F}_{q^m}^{k\times n}$ is a matrix which has minimum column rank Moore decomposition $X = A_{\text{Moore}} + A$, where A_{Moore} is a Moore matrix, and A has column rank s. Then, any other minimum column rank Moore decomposition $X = B_{\text{Moore}} + B$ satisfies that $\text{supp}_{\text{Gr}}(A) = \text{supp}_{\text{Gr}}(B)$.*

Proof. Let A have Grassmann support U, and B have Grassmann support V. I.e., we can write $A = A'U$ and $B = B'V$ with $U, V \in \mathbb{F}_q^{s\times n}$ of full rank. Let $E \in \mathbb{F}_q^{(n-s)\times n}$ be a parity check matrix for $\langle V\rangle$. Then,

$$B_{\text{Moore}}E^T = XE^T - BE^T = XE^T = A_{\text{Moore}}E^T + AE^T,$$

which yields

$$(B_{\text{Moore}} - A_{\text{Moore}})E^T = AE^T.$$

Since E is a matrix over $\mathbb{F}_q$, $(B_{\text{Moore}} - A_{\text{Moore}})E^T$ is a Moore matrix, therefore the matrix AE^T must be a Moore matrix as well. This gives that $(AE^T)_i = (A_1E^T)^{([i-1])} = A_1^{([i-1])}E^T$ for $i = 2, \ldots, k$. Since A itself is not necessarily a Moore matrix, row i of A must be of the form $A_i \in A_1^{([i-1])} + \ker(E)$, for $i = 1, \ldots, k$. Then, we can write

$$A = \underbrace{\begin{pmatrix} A_1 \\ A_1^{([1])} \\ \vdots \\ A_1^{([k-1])} \end{pmatrix}}_{\bar{A}} + \underbrace{\begin{pmatrix} \kappa_1 \\ \kappa_2 \\ \vdots \\ \kappa_k \end{pmatrix}}_{\kappa' V},$$

for $\kappa_1, \ldots, \kappa_k \in \ker(E) = \langle V\rangle$ and $\kappa' \in \mathbb{F}_{q^m}^{k\times s}$. If we let $F \in \mathbb{F}_q^{(n-s)\times n}$ be a parity check matrix for $\langle U\rangle$, then $AF^T = A'UF^T = 0$ and hence in particular $A_1F^T = 0$. Since F is a matrix over $\mathbb{F}_q$, we also get $A_1^{([i])}F^T = 0$ for $i = 1, \ldots, k-1$. Hence,

$$0 = AF^T = \bar{A}F^T + \kappa' VF^T = \kappa' VF^T.$$

Since $X = (A_{\text{Moore}} + \bar{A}) + \kappa' V$ is also a Moore decomposition of X, then the column rank of $\kappa' V$ must be equal to s and so $\langle V \rangle = \langle \kappa' V \rangle$. Thus,

$$\langle V \rangle F^T = 0,$$

and therefore, $\langle V \rangle = \langle U \rangle$, so the Grassmann supports of A and B are the same. □

Theorem 3.10. *Let $M \in \mathbb{F}_{q^m}^{k \times n}$ be a Moore matrix and $X \in \mathbb{F}_{q^m}^{k \times n}$ be of column rank s, where s is the rank of the non-Moore component in a minimum column rank Moore decomposition of X. Then, we have*

$$\sum_{i=0}^{s} \langle M + X \rangle^{([i])} = \sum_{i=0}^{s} \langle M \rangle^{([i])} + \text{supp}_{\text{Gr}}(X).$$

Proof. Let $U \in \mathbb{F}_q^{s \times n}$ be the Grassmann support of X. Moreover, let X_i, M_i denote the ith row of X and M respectively, and let

$$X' = \begin{pmatrix} X_1^{([1])} - X_2 \\ X_2^{([1])} - X_3 \\ \vdots \\ X_{k-1}^{([1])} - X_k \end{pmatrix}, M^* = \begin{pmatrix} M_1 \\ M_1^{([1])} \\ \vdots \\ M_1^{([k+s-1])} \end{pmatrix}, X^* = \left(\begin{array}{c} X_1 \\ X_1^{([1])} \\ \vdots \\ X_1^{([s-1])} \\ \hline X_1^{([s])} \\ X_2^{([s])} \\ \vdots \\ X_k^{([s])} \end{array}\right).$$

Then the space $\sum_{i=0}^{s} \langle M + X \rangle^{([i])}$ is generated by the row span of

$$\begin{pmatrix} M + X \\ (M + X)^{([1])} \\ \vdots \\ (M + X)^{([s])} \end{pmatrix} = \tilde{S} \begin{pmatrix} M^* + X^* \\ X' \\ \vdots \\ (X')^{([s-1])} \end{pmatrix}, \tag{9}$$

for a suitable row transformation matrix $\tilde{S}$. Since $U \in \mathbb{F}_q^{s \times n}$ we have $U^{([i])} = U$ for $i \geq 0$. It follows that the rows of X' are elements of $\langle U \rangle$, which implies that the Grassmann support $\langle U' \rangle$ of X' is a subspace of $\langle U \rangle$ and hence that X' has column rank $s' \leq s$. By Theorem 3.7,

$$\sum_{i=0}^{s'-1} \langle X' \rangle^{([i])} = \sum_{i=0}^{s-1} \langle X' \rangle^{([i])} = \langle U' \rangle \subseteq \langle U \rangle.$$

We now want to show that $\langle U' \rangle = \langle U \rangle$. Suppose for the sake of contradiction that

the rank of U' is strictly smaller than s. We write X as a Moore decomposition

$$X = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_k \end{pmatrix} = \begin{pmatrix} X_1 \\ X_1^{([1])} \\ \vdots \\ X_1^{([k-1])} \end{pmatrix} + \underbrace{\begin{pmatrix} 0 \\ X_2 - X_1^{([1])} \\ \vdots \\ X_k - X_1^{([k-1])} \end{pmatrix}}_{X''}.$$

We note that $X_{i+1} - X_i^{[1]} \in \langle U' \rangle$ for $i = 1, ..., k-1$. Starting from the first non-zero row of X'', it follows that

$$(X_2 - X_1^{([1])})^{([1])} = X_2^{([1])} - X_1^{([2])} \in \langle U' \rangle$$

which implies

$$\begin{aligned} & X_2^{([1])} - X_1^{([2])} - (X_2^{([1])} - X_3) \in \langle U' \rangle \\ \iff \quad & X_3 - X_1^{([2])} \in \langle U' \rangle. \end{aligned}$$

We recognize this as the second non-zero row of X''. Continuing in this fashion, we can obtain that every row of X'' must belong to U'. Hence, X'' has column rank at most $s' < s$. However, this contradicts the fact that the minimal column rank Moore decomposition has non-Moore part with column rank s. Therefore, by Proposition 3.9, U' has rank s and we have $\langle U' \rangle = \langle U \rangle$.

Hence, we have shown that the row space of the second matrix in (9) is equal to the row space of

$$\begin{pmatrix} M^* + X^* \\ U \end{pmatrix}$$

which is in turn equal to the row space of

$$\begin{pmatrix} M^* \\ U \end{pmatrix},$$

because we can cancel X^* by taking suitable elements of $\langle U \rangle$, since $\langle X^* \rangle \subseteq \langle U' \rangle = \langle U \rangle$. This implies the statement. □

Lemma 3.11. *Let $X \in \mathbb{F}_{q^m}^{k \times n}$ have minimum column rank Moore decomposition, $X = X_{\text{Moore}} + Z$. Then,*

$$\text{supp}_{\text{Gr}}(X_{\text{Moore}}) + \text{supp}_{\text{Gr}}(Z) = \text{supp}_{\text{Gr}}(X).$$

In particular, $\text{colrk}(X_{\text{Moore}}) \leq \text{colrk}(X)$.

Proof. Define $\ell := \max(\mathrm{colrk}(X), \mathrm{colrk}(X_{\mathrm{Moore}}))$. Using Theorems 3.7 and 3.10, we have

$$\begin{aligned}
\mathrm{supp}_{\mathrm{Gr}}(X) &= \sum_{i=0}^{\ell} \langle X \rangle^{([i])} \\
&= \sum_{i=0}^{\ell} \langle X_{\mathrm{Moore}} + Z \rangle^{([i])} \\
&= \sum_{i=0}^{\ell} \langle X_{\mathrm{Moore}} \rangle^{([i])} + \mathrm{supp}_{\mathrm{Gr}}(Z) \\
&= \mathrm{supp}_{\mathrm{Gr}}(X_{\mathrm{Moore}}) + \mathrm{supp}_{\mathrm{Gr}}(Z).
\end{aligned}$$

□

Corollary 3.12. *Let $M \in \mathbb{F}_{q^m}^{k \times N}$ be a Moore matrix and X be of column rank t with minimum column rank Moore decomposition $X = X_{\mathrm{Moore}} + Z$, where $\mathrm{colrk}(Z) = s$. Suppose that $d^{\mathrm{R}}_{\min}(\langle M \rangle) \geq s + t + 2$. Then, all elements of rank one in*

$$\sum_{i=0}^{s} \langle M + X \rangle^{([i])},$$

belong to $\mathrm{supp}_{\mathrm{Gr}}(X)$. Moreover, if $s = t$, the elements of rank one exactly span $\mathrm{supp}_{\mathrm{Gr}}(X) = \mathrm{supp}_{\mathrm{Gr}}(Z)$.

Proof. Let $\mathcal{U}$ be the subspace spanned by all elements of rank one in

$$\sum_{i=0}^{s} \langle M + X \rangle^{([i])}.$$

From Lemma 3.11, if $X = X_{\mathrm{Moore}} + Z$, is a minimum column rank decomposition, then we know that $\mathrm{supp}_{\mathrm{Gr}}(Z) \subseteq \mathrm{supp}_{\mathrm{Gr}}(X)$. Let $H \in \mathbb{F}_q^{(n-t) \times n}$ be parity check matrix for $\mathrm{supp}_{\mathrm{Gr}}(X)$. From Lemma 2.4, we have

$$\begin{aligned}
d^{\mathrm{R}}_{\min}\left(\sum_{i=0}^{s} \langle M + X \rangle^{([i])} H^T \right) &= d^{\mathrm{R}}_{\min}\left(\sum_{i=0}^{s} \langle M \rangle^{([i])} H^T \right) \\
&\geq (s + t + 2) - s - t \\
&= 2.
\end{aligned}$$

Since H is a matrix over $\mathbb{F}_q$, we get $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{x}) \leq \mathrm{wt}_{\mathrm{R}}(\boldsymbol{x}H)$, and therefore we must have that $\mathcal{U} \subseteq \mathrm{supp}_{\mathrm{Gr}}(X)$. By Theorem 3.10, $\mathrm{supp}_{\mathrm{Gr}}(Z) \subseteq \mathcal{U}$ and if $s = t$ then $\mathrm{supp}_{\mathrm{Gr}}(Z) = \mathrm{supp}_{\mathrm{Gr}}(X)$. Therefore we have

$$\mathrm{supp}_{\mathrm{Gr}}(Z) = \mathcal{U} = \mathrm{supp}_{\mathrm{Gr}}(X).$$

□

To set up our attack in Section 4, we need to find the elements of rank one in a linear rank metric code efficiently. To accomplish this, we only need to find the codewords that have all coordinates in $\mathbb{F}_q$ (all other rank one codewords are multiples of these). The following lemma shows how these codewords in $\mathbb{F}_q^n$ can be computed.

Lemma 3.13. *Let $G \in \mathbb{F}_{q^m}^{k\times n}$ be in reduced row echelon form and denote by G_i the i-th row of G. Then the solutions to*

$$\sum_{i=1}^{k} a_i(G_i^{([1])} - G_i) = 0, \tag{10}$$

for variables $a_i \in \mathbb{F}_q$, represent the codewords of $\langle G\rangle$ in $\mathbb{F}_q^n$.

Proof. Any codeword can be written as an $\mathbb{F}_{q^m}$-linear combination of the rows of G. Since all rows of G have their pivot equal to 1, a codeword with entries only in $\mathbb{F}_q$ needs to be an $\mathbb{F}_q$-linear combination of the rows. Thus, we get that any codeword in $\mathbb{F}_q^n$ can be written as $\sum_{i=1}^{k} a_iG_i$ for some $a_i \in \mathbb{F}_q$. Furthermore, we know that

$$\boldsymbol{v} \in \mathbb{F}_q^n \iff \boldsymbol{v}^{([1])} - \boldsymbol{v} = 0,$$

hence

$$\sum_{i=1}^{k} a_iG_i \in \mathbb{F}_q^n \iff \sum_{i=1}^{k} a_i(G_i^{([1])} - G_i) = 0.$$

□

When expanded over $\mathbb{F}_q$, Equation (10) gives rise to a linear system of equations with k variables, which can efficiently be solved with standard methods.

4 Cryptanalysis of the GPT Cryptosystem

In this section we explain our new attack to break the GPT cryptosystem, as defined in Subsection 2.2. Our attack extends Overbeck's attack to cryptanalyze the system for all parameters. In Section 5, we show how this same idea can be used to cryptanalyze the GGPT variant.

Recall that the public key generator matrix is of the form

$$G_{\text{pub}} := SG + X \in \mathbb{F}_{q^m}^{k\times n},$$

where G is a generator matrix of a Gabidulin code $\text{Gab}_{n,k}(\boldsymbol{\alpha})$, $X \in \mathbb{F}_{q^m}^{k\times n}$ is a matrix of column rank t, and $S \in \text{GL}_k(\mathbb{F}_{q^m})$.

Note that, as an attacker, we do not have a priori knowledge of the parameter s (the column rank of the non-Moore part in the minimal column rank Moore decomposition of X). We can generally assume $s = t$, or else start with $s = 1$ and increase the value up to t until the attack succeeds.

Theorem 4.1. *Consider a GPT cryptosystem as defined in Subsection 2.2, with public key generator matrix* $G_{\text{pub}} = SG + X \in \mathbb{F}_{q^m}^{k\times n}$. *Let* $S^{-1}X = X_{\text{Moore}} + Z$ *be a minimal column rank Moore decomposition with* $s = \text{colrk}(Z)$. *Suppose an adversary can find a full rank matrix* $U \in \mathbb{F}_q^{s'\times n}$ *for* $s \leq s' \leq t$ *satisfying*

$$\text{supp}_{\text{Gr}}(Z) \subseteq \langle U \rangle \subseteq \text{supp}_{\text{Gr}}(X),$$

then an encrypted message from a public key of the form (3) *can be recovered in polynomial time.*

Proof. Let $H \in \mathbb{F}_q^{(n-s')\times n}$ be a parity check matrix for $\langle U \rangle$. Applying H to the public key generator matrix yields

$$G_{\text{pub}}H^T = (SG + X)H^T = S(G + X_{\text{Moore}})H^T.$$

From Lemma 3.11 we know that $\text{colrk}(X_{\text{Moore}}) \leq t$. Then, from Lemma 2.4, it follows that $\langle G + X_{\text{Moore}} \rangle$ has minimum rank distance at least $n - k + 1 - t$, and that $\langle G + X_{\text{Moore}}H^T \rangle$ has minimum rank distance at least $n - k + 1 - (t + s')$. Moreover, $GH^T + X_{\text{Moore}}H^T$ is a Moore matrix.

From the minimum distance we know that there are $n-(t+s')$ independent columns in this matrix, which generate a Gabidulin code of minimum distance $n-(t+s')-k+1$, $\text{Gab}_{n-(t+s'),k}(\boldsymbol{\gamma})$, for some $\boldsymbol{\gamma} \in \mathbb{F}_{q^m}^{n-(t+s')}$. From Subsection 2.1, we can recover a decoding algorithm for $\text{Gab}_{n-(t+s'),k}(\boldsymbol{\gamma})$ with respect to the submatrix formed by these $n-(t+s')$ columns. The error correction capability of $\text{Gab}_{n-(t+s'),k}(\boldsymbol{\gamma})$ is

$$\left\lfloor \frac{n-(t+s')-k}{2} \right\rfloor = \left\lfloor t' - \frac{t+s'}{2} \right\rfloor \geq t' - t \geq \text{rk}(\boldsymbol{e}) \geq \text{rk}(\boldsymbol{e}H^T),$$

where the last inequality follows from the fact that H is a matrix over $\mathbb{F}_q$. For an encrypted message $\boldsymbol{m}(SG + X) + \boldsymbol{e}$, we have

$$(\boldsymbol{m}(SG + X) + \boldsymbol{e})H^T = \boldsymbol{m}S(GH^T + X_{\text{Moore}}H^T) + \boldsymbol{e}H^T.$$

When we restrict this to the above chosen independent columns, we can uniquely decode in the respective code $\text{Gab}_{n-(t+s'),k}(\boldsymbol{\gamma})$ and can therefore recover $\boldsymbol{m}$. □

We can now use the previous result to attack and break the GPT cryptosystem.

Corollary 4.2. *Consider a GPT cryptosystem as defined in Subsection 2.2 with public key generator matrix* $G_{\text{pub}} = SG + X \in \mathbb{F}_{q^m}^{k\times n}$. *For any such cryptosystem, an encrypted message can be recovered in polynomial time.*

Proof. As before, let $S^{-1}X = X_{\text{Moore}} + Z$ be a minimal column rank Moore decomposition. Denote by s the column rank of Z. We first note that $d_{\min}^{\text{R}}(\langle G \rangle) \geq s + t + 2$, since

$$\frac{d_{\min}^{\text{R}}(\langle G \rangle) - 1}{2} \geq \left\lfloor \frac{n-k}{2} \right\rfloor = t' > t \geq \frac{s+t}{2}.$$

By Corollary 3.12, all the elements of rank one in $\sum_{i=0}^{s}\langle G+X\rangle^{([i])}$ belong to the Grassmann support of X. With Lemma 3.13 we can find a basis matrix $U \in \mathbb{F}_q^{s'\times n}$ for these elements of rank one in polynomial time. We have $\langle U\rangle \subseteq \mathrm{supp}_{\mathrm{Gr}}(X)$. On the other hand, by Theorem 3.10, $\mathrm{supp}_{\mathrm{Gr}}(Z) \subseteq \sum_{i=0}^{s}\langle G+X\rangle^{([i])}$. Thus, we also have $\mathrm{supp}_{\mathrm{Gr}}(Z) \subseteq \langle U\rangle$. Therefore we can use Theorem 4.1 to recover the encrypted message. □

5 Cryptanalysis of GGPT Variants

In this section we adapt our attack to break the GGPT cryptosystem, as defined in Subsection 2.2. To do so we will consider two variants of the GGPT separately. However, in both subsections we will consider a public key generator matrix of the form

$$\hat{G}_{\mathrm{pub}} := S[X \mid G]\sigma \in \mathbb{F}_{q^m}^{k\times(n+\hat{t})},$$

where G is a generator matrix of some Gabidulin code $\mathrm{Gab}_{n,k}(\boldsymbol{\alpha})$, $X \in \mathbb{F}_{q^m}^{k\times\hat{t}}$ is a matrix of column rank $\hat{t}$, $S \in \mathrm{GL}_k(\mathbb{F}_{q^m})$, and $\sigma \in \mathrm{GL}_{n+\hat{t}}(\mathbb{F}_q)$.

5.1 Smart Approach Variant

Recall from Subection 2.3 that we can put the extended matrix into the form

$$G'_{\mathrm{ext}} = \tilde{S}'\left(\begin{array}{c|c} X^* & G^* \\ X^{**} & 0 \end{array}\right)\sigma.$$

Rashwan et al. in [18] proposed what they call the *Smart Approach (SA)*. In this setting, they note that if $X \in \mathbb{F}_{q^m}^{k\times\hat{t}}$ is constructed from a Moore matrix of column rank a and a non-Moore component of column rank $\hat{t}-a$, then X^{**} will have rank $\hat{t}-a$. The paper gives no suggestions for design parameters of such a system. However, one implicit advantage of this construction is the ability to predict the rank of X^{**}, and therefore to be able to reduce the public key by choosing a smaller designed error matrix.

In the SA variant we can write $X = X_{\mathrm{Moore}} + Z$ as a minimal column rank Moore decomposition, where X_{Moore} has column rank a and Z has column rank $\hat{t}-a$. We can then rewrite

$$\hat{G}_{\mathrm{pub}} = \underbrace{S[X_{\mathrm{Moore}} \mid G]\sigma}_{M} + \underbrace{S[Z \mid 0]\sigma}_{X'}. \tag{11}$$

X' is a matrix of column rank $\hat{t}-a$ and $S^{-1}M$ is a Moore matrix generating a code with minimum rank distance at least $n-k+1$.

Theorem 5.1. *Consider a GGPT cryptosystem as defined above. Suppose an adversary can find a matrix $U' \in \mathbb{F}_q^{(\hat{t}-a)\times(\hat{t}+n)}$, such that $\langle U'\rangle = \mathrm{supp}_{\mathrm{Gr}}([Z \mid 0]\sigma) = \mathrm{supp}_{\mathrm{Gr}}(X')$. Then an encrypted message from a public key of the form (5) can be recovered in polynomial time.*

Proof. We note that U' must be of the form $U' = [U \mid 0]\sigma$, where $U \in \mathbb{F}_q^{(\hat{t}-a)\times\hat{t}}$ is such that $\mathrm{supp}_{\mathrm{Gr}}(Z) = \langle U \rangle$. Let $H_U \in \mathbb{F}_q^{a\times\hat{t}}$ be a parity check matrix for U. A parity check matrix $H_{U'} \in \mathbb{F}_q^{(a+n)\times(\hat{t}+n)}$ for U' must be of the form

$$(H_{U'})^T = \sigma^{-1} \left[\begin{array}{c|c} H_U^T & 0_{\hat{t}\times n} \\ \hline 0_{n\times a} & I_n \end{array}\right] A,$$

for some $A \in \mathrm{GL}_{n+a}(\mathbb{F}_q)$.

We compute

$$\begin{aligned} \hat{G}_{\mathrm{pub}}(H_{U'})^T &= S[X_{\mathrm{Moore}} \mid G]\sigma(H_{U'})^T + S[Z \mid 0]\sigma(H_{U'})^T \\ &= S[X_{\mathrm{Moore}} \mid G] \left[\begin{array}{c|c} H_U^T & 0_{\hat{t}\times n} \\ \hline 0_{n\times a} & I_n \end{array}\right] A \\ &= S[X_{\mathrm{Moore}} H_U^T \mid G]A. \end{aligned}$$

$[X_{\mathrm{Moore}} H_U^T \mid G]A$ is again a Moore matrix, generating a code of minimum distance at least $n-k+1$. Hence, we can find n independent columns of $\hat{G}_{\mathrm{pub}}(H_{U'})^T$ which will form a Gabidulin code of minimum distance $n-k+1$. Denote these columns by $\boldsymbol{i} = (i_1, \dots i_n)$ and the corresponding submatrix by $G_{\boldsymbol{i}}$. From Section 2.1, we can recover a decoding algorithm for $\langle G_{\boldsymbol{i}} \rangle$ with respect to $G_{\boldsymbol{i}}$.

We note that if $\boldsymbol{e}$ is an error of rank at most t', and we denote by $\boldsymbol{e'}$ the subvector of $\boldsymbol{e}(H_{U'})^T$ corresponding to columns $\boldsymbol{i}$, then

$$\mathrm{rk}(\boldsymbol{e'}) \leq \mathrm{rk}(\boldsymbol{e}(H_{U'})^T) \leq \mathrm{rk}(\boldsymbol{e}) \leq t'.$$

If we apply $H_{U'}$ to an encrypted message of the form $\boldsymbol{m}\hat{G}_{\mathrm{pub}} + \boldsymbol{e}$, we obtain

$$\boldsymbol{m}\hat{G}_{\mathrm{pub}}(H_{U'})^T + \boldsymbol{e}(H_{U'})^T.$$

Restricting to the coordinates $\boldsymbol{i}$, we obtain

$$\boldsymbol{m}G_{\boldsymbol{i}} + \boldsymbol{e'},$$

which we can decode in the code $\langle G_{\boldsymbol{i}} \rangle$ to recover $\boldsymbol{m}$, since the error correction capability of $\langle G_{\boldsymbol{i}} \rangle$ is $t' \geq \mathrm{rk}(\boldsymbol{e'})$. □

Corollary 5.2. *Consider a GGPT cryptosystem as defined above. If*

$$\hat{t} - a < \frac{n-k-1}{2}$$

we can recover an encrypted message in polynomial time.

Proof. Recall that

$$\hat{G}_{\mathrm{pub}} = \underbrace{S[X_{\mathrm{Moore}} \mid G]\sigma}_{M} + \underbrace{S[Z \mid 0]\sigma}_{X'}$$

is a minimum column rank Moore decomposition. Then $S^{-1}\hat{G}_{\text{pub}} = S^{-1}M + S^{-1}X'$ is also a minimal column rank Moore decomposition. $S^{-1}M$ is a Moore matrix generating a code of minimum rank distance at least $n-k+1$. Since, by the condition of this corollary,

$$n-k+1 \geq 2(\hat{t}-a)+2,$$

it follows from Corollary 3.12 that all elements of rank one in

$$\sum_{i=0}^{\hat{t}-a} \langle \hat{G}_{\text{pub}} \rangle^{([i])} = \sum_{i=0}^{\hat{t}-a} \langle S^{-1}\hat{G}_{\text{pub}} \rangle^{([i])} = \sum_{i=0}^{\hat{t}-a} \langle S^{-1}M + S^{-1}X' \rangle^{([i])}$$

span the space $\text{supp}_{\text{Gr}}(X') = \text{supp}_{\text{Gr}}([Z \mid 0]\sigma)$. We can use Lemma 3.13 to find these elements of rank one, and obtain $U' \in \mathbb{F}_q^{(\hat{t}-a)\times(\hat{t}+n)}$ such that $\langle U' \rangle = \text{supp}_{\text{Gr}}(X')$. Then we can use Theorem 5.1 to recover the message. □

The following example illustrates a case when Overbeck's attack fails, but our attack recovers the encrypted message.

Example 5.3. Let $q=2$, $n=8$, $k=3$, $\hat{t}=3$, $a=1$ and $g_1,\ldots,g_8 \in \mathbb{F}_{2^8}$ linearly independent over $\mathbb{F}_2$. Consider the generator matrix of a Gabidulin code

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_8 \\ g_1^{([1])} & g_2^{([1])} & \cdots & g_8^{([1])} \\ g_1^{([2])} & g_2^{([2])} & \cdots & g_8^{([2])} \end{pmatrix},$$

and, for some $x \in \mathbb{F}_{2^8} \backslash \mathbb{F}_2$, the matrices

$$X_{\text{Moore}} = \begin{pmatrix} x & 0 & 0 \\ x^{([1])} & 0 & 0 \\ x^{([2])} & 0 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Let

$$X = X_{\text{Moore}} + Z$$

and the public key generator matrix be

$$\hat{G}_{\text{pub}} = [X \mid G] = \left(\begin{array}{ccc|ccc} x & 1 & 1 & g_1 & g_2 & \cdots & g_8 \\ x^{([1])}+1 & 0 & 1 & g_1^{([1])} & g_2^{([1])} & \cdots & g_8^{([1])} \\ x^{([2])}+1 & 1 & 0 & g_1^{([2])} & g_2^{([2])} & \cdots & g_8^{([2])} \end{array}\right).$$

For simplicity we let $S = I_3$ and $\sigma = I_{11}$. We choose $u=1$ and construct G_{ext}, which can be put in the form

$$G'_{\text{ext}} = \left(\begin{array}{ccc|ccc} x & 0 & 0 & g_1 & g_2 & \cdots & g_8 \\ x^{([1])} & 0 & 0 & g_1^{([1])} & g_2^{([1])} & \cdots & g_8^{([1])} \\ x^{([2])} & 0 & 0 & g_1^{([2])} & g_2^{([2])} & \cdots & g_8^{([2])} \\ x^{([3])} & 0 & 0 & g_1^{([3])} & g_2^{([3])} & \cdots & g_8^{([3])} \\ 1 & 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 1 & 0 & \ldots & 0 & 0 \end{array}\right) = \left(\begin{array}{c|c} X^* & G^* \\ X^{**} & 0 \end{array}\right)$$

by a suitable row transformation. Here Overbeck's attack fails, because X^{**} does not have full rank. On the other hand, our attack succeeds, since we can directly recover the elements of rank one as $\langle [X^{**} \mid 0] \rangle = \langle [Z \mid 0] \rangle$. Thus we can use Theorem 5.1 and recover any encrypted message.

5.2 Loidreau's GGPT Variant

As already mentioned in Subsection 2.3, in Loidreau's GGPT variant [13] the designed error matrix, $X \in \mathbb{F}_{q^m}^{k \times \hat{t}}$, is a randomly chosen matrix of rank $a < \hat{t}/(n-k)$. We can assume that X has column rank $\hat{t}$. In this case, to find the Grassmann support of X with the help of Theorem 3.7, we need to go up to the $(\hat{t}-1)$-st Frobenius power. But, since

$$\hat{t} - 1 > a(n-k) - 1 \geq n - k - 1,$$

we get that

$$\sum_{i=0}^{\hat{t}-1} G^{([i])} = \sum_{i=0}^{n-k-1} G^{([i])} = \mathbb{F}_{q^m}^n,$$

hence the elements of rank one cannot help us reconstruct the Grassmann support of X. Thus the attack of Subsection 5.1 would not succeed.

However, in this case, we can still use the idea of locating the elements of rank one; but now we want to recover the elements of the Gabidulin part of the code, instead of the Grassmann support of X. The strategy is effectively the same, although we must make some assumptions on the behavior of X and random subcodes of Gabidulin codes.

First, we note that there is a suitable row transformation, T, so that

$$T\hat{G}_{\text{pub}} = \left(\begin{array}{c|c} X^* & G^* \\ 0 & G^{**} \end{array} \right) \sigma, \tag{12}$$

where $X^* \in \mathbb{F}_{q^m}^{a \times \hat{t}}$ is a matrix with the same row span as X, and G^* and G^{**} are matrices which span subcodes of $\langle G \rangle$. One can easily see that $\langle [X^* \mid G^*]\sigma \rangle$ and $\langle [0 \mid G^{**}]\sigma \rangle$ intersect trivially. Our strategy will be to use the purely Gabidulin part $[0 \mid G^{**}]$ to generate a parity check matrix for $[X^* \mid 0]$.

We will now state the assumptions that we will use in our attack. These assumptions are justified with experimental results in Table 1.

Assumption 1. *Let $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a Gabidulin code, and $\mathcal{B} \subset \langle G \rangle$ be a random subspace of $\langle G \rangle$ of codimension a. Set*

$$\ell = \left\lceil \frac{n}{k-a} \right\rceil. \tag{13}$$

With high probability, we have

$$\sum_{i=0}^{\ell-1} \mathcal{B}^{([i(k-a)])} = \mathbb{F}_{q^m}^n. \tag{14}$$

m	n	k	a	$\hat{t}$	Assumption 1	Assumption 2
24	24	12	3	40	~ 1	~ 1
24	24	12	4	52	$\sim .998$	~ 1

Table 1: Experimental results for Assumptions 1 and 2: Probabilities of success in 1000 trials for $q = 2$.

The value of ℓ in (13) is the smallest possible value for which we can obtain equality in (14). One could choose ℓ larger than in (13), which we will remark on in the end of this section.

Since we can expect a random matrix whose rank is small relative to the dimension of the ambient space to not contain elements of rank one, we make the additional assumption:

Assumption 2. *Let $X \in \mathbb{F}_{q^m}^{k\times\hat{t}}$ be a random matrix of rank a. For ℓ given in* (13)*, if $\ell a \ll \hat{t}$, then with high probability,*

$$\sum_{i=0}^{\ell-1}\langle X\rangle^{([i(k-a)])}$$

contains no elements of rank one.

Theorem 5.4. *Let $S \in \mathrm{GL}_k(\mathbb{F}_{q^m})$, $\sigma \in \mathrm{GL}_{n+\hat{t}}(\mathbb{F}_q)$, $G \in \mathbb{F}_{q^m}^{k\times n}$, and $X \in \mathbb{F}_{q^m}^{k\times\hat{t}}$ be of rank a, and consider Loidreau's GGPT variant with public key*

$$\hat{G}_{\mathrm{pub}} = S[X \mid G]\sigma.$$

If Assumptions 1 and 2 are true, then we can break the Loidreau GGPT variant in polynomial time with high probability.

Proof. Let ℓ be as in (13) and $T\hat{G}_{\mathrm{pub}}$ as in (12). Consider the matrix

$$G''_{\mathrm{ext}} := \begin{pmatrix} \hat{G}_{\mathrm{pub}} \\ \hat{G}_{\mathrm{pub}}^{([k-a])} \\ \vdots \\ \hat{G}_{\mathrm{pub}}^{([(k-a)(\ell-1)])} \end{pmatrix} = \tilde{S}\underbrace{\left(\begin{array}{c} (X^* \mid G^*) \\ (X^* \mid G^*)^{([k-a])} \\ \vdots \\ (X^* \mid G^*)^{([(k-a)(\ell-1)])} \\ \hline (0 \mid G^{**}) \\ (0 \mid G^{**})^{([k-a])} \\ \vdots \\ (0 \mid G^{**})^{([(k-a)(\ell-1)])} \end{array}\right)}_{\bar{G}}\sigma.$$

Since $\langle G^{**}\rangle$ is a subcode of $\langle G\rangle$ of codimension a, by Assumption 1, we have with high probability,

$$\sum_{i=0}^{\ell-1}\langle G^{**}\rangle^{([(k-a)i])} = \mathbb{F}_{q^m}^n.$$

Then, the bottom submatrix of $\bar{G}$ has the same row span as $[0 \mid I_n]$, and hence, by using elementary operations, we can eliminate the second component of every row in the top submatrix of $\bar{G}$. Then, the space generated by the rows of G''_{ext} is the same as that generated by

$$G'''_{\text{ext}} = \left(\begin{array}{c|c} X^* & 0 \\ (X^*)^{([k-a])} & 0 \\ \vdots & \vdots \\ (X^*)^{([(k-a)(\ell-1)])} & 0 \\ 0 & I_n \end{array} \right) \sigma.$$

By Assumption 2, with high probability we have that

$$\sum_{i=0}^{\ell-1} \langle X^* \rangle^{([(k-a)i])}$$

contains no elements of rank one, and therefore all elements of rank one in $\langle G''_{\text{ext}} \rangle = \langle G'''_{\text{ext}} \rangle$ must belong to $\langle [0 \mid I_n] \rangle \sigma$. With the help of Lemma 3.13 we can recover a matrix $U \in \mathbb{F}_q^{n \times (\hat{t}+n)}$ which is a basis for $\langle [0 \mid I_n] \rangle \sigma$. Then, any parity check matrix $H_U \in \mathbb{F}_q^{\hat{t} \times (n+\hat{t})}$ for $\langle [0 \mid I_n] \rangle \sigma$ must have the form

$$H_U^T = \sigma^{-1} \left[\begin{array}{c} A \\ 0 \end{array} \right] \in \mathbb{F}_q^{(n+\hat{t}) \times \hat{t}},$$

where $A \in \mathrm{GL}_{\hat{t}}(\mathbb{F}_q)$. It follows that, if we compute

$$\hat{G}_{\text{pub}} H_U^T = S[X \mid G] \sigma H_U^T = SXA \in \mathbb{F}_{q^m}^{k \times \hat{t}},$$

then there exists a unique matrix $V = [A^{-1} \mid 0] \sigma \in \mathbb{F}_q^{\hat{t} \times (n+\hat{t})}$ such that

$$\hat{G}_{\text{pub}} H_U^T V = SXAV = S[X \mid 0] \sigma.$$

We can find the matrix V by observing that

$$(\hat{G}_{\text{pub}} - \hat{G}_{\text{pub}} H_U^T V) H_U^T = S[0 \mid G] \sigma H_U^T = 0. \tag{15}$$

This gives a linear system of equations with $\hat{t}(n+\hat{t})$ variables and $k \times \hat{t}$ equations over $\mathbb{F}_{q^m}$. Since the variables can only take values in $\mathbb{F}_q$, we can expand each equation into m equations over $\mathbb{F}_q$, obtaining a system of $km\hat{t}$ equations and $\hat{t}(n+\hat{t})$ variables over $\mathbb{F}_q$. Hence, we can solve this system of equations if $km \geq n + \hat{t}$ (which is always satisfied).

Let $H_V \in \mathbb{F}_{q^m}^{n \times (n+\hat{t})}$ be any dual matrix for V. Then, H_V has the form

$$H_V^T = \sigma^{-1} \left[\begin{array}{c} 0 \\ B \end{array} \right],$$

for some $B \in \mathrm{GL}_n(\mathbb{F}_q)$. Therefore,

$$\hat{G}_{\text{pub}} H_V^T = S[X \mid G] \sigma H_V^T = SGB \in \mathbb{F}_{q^m}^{k \times n}$$

is a Gabidulin code of minimum distance $n-k+1$, from which we can recover a decoding algorithm, as explained in Subsection 2.1. If we receive an encrypted message of the form

$$\boldsymbol{m}\hat{G}_{\text{pub}} + \boldsymbol{e},$$

we can apply H_V, obtaining

$$\boldsymbol{m}SGB + \boldsymbol{e}H_V^T.$$

Since

$$\text{rk}(\boldsymbol{e}H_V^T) \leq \text{wt}_{\text{R}}(\boldsymbol{e}) \leq t',$$

we can recover the encrypted message, $\boldsymbol{m}$, from the recovered decoding algorithm with respect to SGB. All the operations required for this attack can be performed in polynomial time. □

We will conclude this section with an example where we analyze our attack against the parameters proposed by Loidreau in [13] in order to resist Overbeck's attack. It turns out that the proposed parameters are not secure against our attack.

Example 5.5. Consider a Loidreau GGPT variant with $q = 2$, $m = n = 24$, $k = 12$, $a = 3$, and $\hat{t} = 40$, i.e. the first set of parameters from Table 1. Assume we, as an attacker, know the public generator matrix $\hat{G}_{\text{pub}} \in \mathbb{F}_{2^{24}}^{12\times 64}$ and received an encrypted message $\boldsymbol{y}$. We compute $\ell = \lceil \frac{24}{12-3} \rceil = 3$ and proceed as follows:

1. We compute $\hat{G}_{\text{pub}}^{([9])}, \hat{G}_{\text{pub}}^{([18])}$ to obtain the extended matrix $G''_{\text{ext}} \in \mathbb{F}_{2^{24}}^{36\times 64}$. This requires at most $1536 = 2 \cdot 12 \cdot 64$ Frobenius powers in $\mathbb{F}_{2^{24}}$. Using a normal basis to represent $\mathbb{F}_{2^{24}}$ over $\mathbb{F}_2$, this can be done very efficiently.

2. We find the elements of rank one in $\langle G''_{\text{ext}} \rangle$, as described in Lemma 3.13. To do so we need to row reduce G''_{ext} and then solve a linear system over $\mathbb{F}_2$ with 36 unknowns and $24 \cdot 64 = 1536$ equations. Then, if Assumptions 1 and 2 hold, we find some basis matrix $U \in \mathbb{F}_2^{24\times 64}$, such that $\langle U \rangle$ contains all these elements of rank one.

3. Compute a parity check matrix H_U for U.

4. We find a matrix $V \in \mathbb{F}_2^{40\times 64}$, solving Equation (15).

5. We compute a parity check matrix $H_V \in \mathbb{F}_2^{64\times 24}$ for V, and compute the product $\hat{G}_{\text{pub}} H_V^T$.

6. We recover a decoding algorithm for the code $\langle \hat{G}_{\text{pub}} H_V^T \rangle$, as described in Lemma 3.13, and decode $\boldsymbol{y}H_V^T$ with this algorithm.

We observe that step 4 above is the most computationally intensive, and therefore we estimate the complexity of our attack based on this step. This is done by solving a $(40 \cdot 64) \times (24 \cdot 12 \cdot 40)$ system over $\mathbb{F}_2$ by Gaussian elimination on the resulting matrix.

This requires on the order of 2^{39} operations over $\mathbb{F}_2$. Implementing the algorithm on a personal computer, we were able to break this system very efficiently.

For the parameters in the second row of the table, we can similarly break the system, albeit with slightly higher complexity due the larger parameters.

6 Conclusion

In this paper, we provide a new attack against cryptosystems based on Gabidulin codes, reconfirming that Gabidulin based cryptosystems are vulnerable from a structural perspective. Our attack generalizes Overbeck's attack, focusing instead on recovering the elements of rank one, rather than the structure of the dual space. One principle advantage of our attack is that it can be extended to cryptanalyze certain variants of the generalized GPT system, which resist the original attacks of Gibson and Overbeck. In particular, we show that the Smart Approach and Loidreau's GGPT variants are vulnerable to this attack.

To the best of the authors' knowledge, attacking a cryptosystem by looking at the elements of rank one is a new approach which may need to be considered for the security of existing and future rank-metric based cryptosystems. As a next step the authors want to use this idea of finding elements of rank one to cryptanalyze the column scrambler variant of [6], which has so far resisted structural attacks.

References

[1] T. P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *Information Theory, IEEE Transactions on*, 49(11):3016–3019, Nov 2003.

[2] F. Chabaud and J. Stern. The cryptographic security of the syndrome decoding problem for rank distance codes. In *Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, pages 368–381, 1996.

[3] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[4] E. M. Gabidulin. Attacks and counter-attacks on the GPT public key cryptosystem. *Designs, Codes and Cryptography*, 48(2):171–177, 2008.

[5] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'91, pages 482–489, Berlin, Heidelberg, 1991. Springer-Verlag.

[6] E. M. Gabidulin, H. Rashwan, and B. Honary. On improving security of GPT cryptosystems. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 1110–1114, June 2009.

[7] P. Gaborit, O. Ruatta, and J. Schrek. On the complexity of the rank syndrome decoding problem. *arXiv*, abs/1301.1026, 2013.

[8] P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor. New results for rank-based cryptography. In *Progress in Cryptology - AFRICACRYPT 2014 - 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings*, pages 1–12, 2014.

[9] J. K. Gibson. Severely denting the Gabidulin version of the McEliece public key cryptosystem. *Des. Codes Cryptography*, 6(1):37–45, July 1995.

[10] M. Giorgetti and A. Previtali. Galois invariance, trace codes and subfield subcodes. *Finite Fields and Their Applications*, 16(2):96–99, 2010.

[11] A.-L. Horlemann-Trautmann and K. Marshall. New criteria for MRD and Gabidulin codes and some rank-metric code constructions. *arXiv:1507.08641*, 2015.

[12] A. Kshevetskiy. Security of GPT-like public-key cryptosystems based on linear rank codes. In *Signal Design and Its Applications in Communications, 2007. IWSDA 2007. 3rd International Workshop on*, pages 143–147, Sept 2007.

[13] P. Loidreau. Designing a rank metric based McEliece cryptosystem. In *Proceedings of the Third International Conference on Post-Quantum Cryptography*, PQCrypto'10, pages 142–152, Berlin, Heidelberg, 2010. Springer-Verlag.

[14] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *Deep Space Network Progress Report*, 44:114–116, January 1978.

[15] K. Morrison. Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes. *IEEE Transactions on Information Theory*, Vol 60(11):1–12, 2014.

[16] A. V. Ourivski and T. Johansson. New technique for decoding codes in the rank metric and its cryptography applications. *Probl. Inf. Transm.*, 38(3):237–246, July 2002.

[17] R. Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *J. Cryptology*, 21(2):280–301, 2008.

[18] H. Rashwan, E. M. Gabidulin, and B. Honary. A smart approach for GPT cryptosystem based on rank codes. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2463–2467, 2010.

[19] V. M. Sidelnikov and S. O. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Mathematics and Applications*, 2:439–444, 1992.

[20] D. Silva and F. R. Kschischang. Fast encoding and decoding of Gabidulin codes. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 2858–2862, June 2009.

[21] A. Wachter-Zeh. Bounds on list decoding of rank-metric codes. *IEEE Transactions on Information Theory*, 59(11):7268–7277, 2013.